COMMUNICATIONS
ALLIANCE LTD

Communications Alliance Submission

to the Attorney General's Department
in response to the

Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021
and associated
Explanatory Paper and
Early Assessment – Regulation Impact Statement

13 December 2021

Contents

Communications Alliance

Communications Alliance is the primary communications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, platform providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to be the most influential association in Australian communications, co-operatively initiating programs that promote sustainable industry development, innovation and growth, while generating positive outcomes for customers and society.

The prime mission of Communications Alliance is to create a co-operative stakeholder environment that allows the industry to take the lead on initiatives which grow the Australian communications industry, enhance the connectivity of all Australians and foster the highest standards of business behaviour.

For more details about Communications Alliance, see http://www.commsalliance.com.au.

1. Introduction

Communications Alliance welcomes the opportunity to make a submission to the Attorney General's Department (AGD) in response to the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021* (Bill), the associated Explanatory Paper (Explanatory Paper) and the Early Assessment – Regulatory Impact Statement (RIS).

Our members take privacy very seriously, and they support a privacy regime that protects the personal information of their customers and the use of customer data.

We acknowledge that the changes brought about by the digital age require ongoing consideration and informed debate from all angles of our society and economy. Our members have invested, and will continue to invest, substantial resources in technological, process and human resource developments to ensure privacy practices remain at the highest level and keep pace with latest societal, technological and legal developments.

As detailed in this submission, we find that there are serious definitional deficiencies within the proposed legislation, along with issues and/or ambiguities relating to scope, proportionality and the timing of consequent implementation. We have made recommendations as to how these problems could be addressed via amendments.

We continue to support a review of the adequacy of the privacy regime and are keen to engage with all stakeholders to ensure that improvements to privacy legislation can benefit all sectors of the economy.

2. Reform Process

2.1. The draft Bill is being released (with a view to being introduced in the Parliament in the short-term) while other relevant reform processes are underway; most notably the review of the *Privacy Act 1988*, which indeed is being consulted on in parallel (albeit for a slightly longer time period) to the Exposure Draft of the Bill.

2.2. Equally relevant in the context of the Bill is the Age Verification Roadmap (AVR) process currently afoot, with the implementation roadmap scheduled to be presented to Government in December 2022.

2.3. The Explanatory Paper to the draft Bill correctly states that "*[a]t present, private sector organisations subject to the Privacy Act must comply with the Act's Australian Privacy Principles (APPs).*"[1]

The Paper goes on to assert that: "*[…] the particular privacy challenges posed by social media and online platforms in complying with the APPs in the online space, it is necessary to provide greater detail and adapt some of the APPs to this context.*"[2]

The only reference provided in the context of this assertion is the Facebook/Cambridge Analytica data harvesting incident in March 2018 which the Office of the Australian Information Commissioner (OAIC) has subsequently initiated legal proceedings in. No further evidence is offered as to the validity of the claim around the particular privacy challenges posed by social media and online platforms in relation to compliance with the Australian Privacy Principles (APPs) and the need for urgent regulatory intervention. Similarly, the RIS does not provide additional insight as to why regulatory intervention is urgently required.

2.4. The RIS indicates that almost all (99%) of the extraordinary costs associated with the implementation of the requirements arising from the Bill relate to age verification and associated parental consent verification – over half a billion dollars, i.e. $526,203,500[3]

[1] p. 4, Explanatory Paper, *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021*, Nov 2021.

[2] ibid

[3] p. 23 Enhancing online privacy and other measures, Early Assessment – Regulation Impact Statement, Oct 2021

(which we believe may to be a very conservative estimate, if the Bill was passed as currently drafted).

2.5. While the Bill describes the measures that are to be contained in a future code, it already sets a prescriptive framework pre-empting, or forcing industry to pre-empt, substantial areas of reform that are still being discussed in the separate process of the Privacy Act Review and are already highlighted as being controversial in the Discussion Paper currently released for public consultation. Those areas include, for example, the definition of 'personal information', requirements for valid 'consent', circumstances in which express consent must be sought and obtained, the scope of operation of transparency requirements in relation to respectively privacy policies and privacy (collection) notices (vs what must be addressed in each), the extent to which use of technical information for differentiated treatment of users will be regulated under the Privacy Act, whether there should be a broad form opt-out option for users of online services, and reasonable bases for exceptions from an opt-out option (i.e., any carve-down for reasonably anticipated or compatible uses or legitimate uses or interests.

2.6. At this stage, it is impossible to assess the effect of any of those or other reforms considered in the Discussion Paper of the Privacy Act Review, and it appears equally impossible to see how industry (or the Privacy Commissioner for that matter) would be able to develop a meaningful, lasting code without knowledge of the detail of those reforms.

2.7. It is important to highlight that, should a code be developed, the true costs of code development – and re-development once the Privacy Act Review has been completed – would be much higher than estimated in the RIS due to the wasted efforts of pre-emptively developing code measures that will almost certainly require substantial reworking once the review of the Act has concluded.

2.8. Consequently, given the lack of evidence that urgent measures are required for social media service and large online platforms and why those have been singled out for a separate reform process, the current other processes underway (Privacy Act Review and AVR) and the extraordinary high costs associated with precisely those mandatory measures (age verification/parental consent) that closely relate to one of the processes on foot (AVR), we believe that consideration of the matters contemplated in the Bill, if required at all in this form, ought to be delayed until the other reform processes have sufficiently processed.

2.9. In addition, we refer to our objections to the age verification and parental consent requirements detailed in Section 4 further below.

3. Definitional issues / scope of services captured

We are concerned about the broad drafting and lack of clarity around a number of terms in the proposed Bill, such as 'OP organisation', 'social media service', 'electronic service', 'large online platform' and 'end-user', which result in an overly broad scope and unnecessarily complex and burdensome (and practically unworkable) requirements for many organisations. These definitions should be more appropriately targeted and clarified so that the organisations considered OP organisations are more aligned to the original intent, as also expressed in the ACCC's Digital Platform Inquiry Final Report (as noted in the Explanatory Paper to the Bill).

<u>Definition of OP organisation</u>

3.1. As previously noted, from the drafting of the obligations in the Bill, and the Explanatory Paper, it appears that the Bill is aimed at addressing "the particular privacy challenges posed by social media and other online platforms that collect a high volume of

personal information or trade in personal information".[4] In other words, the legislative intent behind the Bill is for it to target consumer-facing service providers who directly interact with individual consumers and who collect the personal information of such consumers.

3.2. However, the definitions proposed in the Bill for 'social media services', 'data brokerage services' and 'large online platforms' are unfortunately broad enough to capture enterprise or business-to-business (B2B) service providers. This would lead to potentially unworkable and impossible obligations being placed on such providers.

3.3. To illustrate, the OP code to be developed under the Bill will impose several enhanced obligations on service providers, including obligations to cease using or disclosing personal information upon request by the individual. The Explanatory Paper provides an example of when an individual may choose to exercise this right – where the individual does not want the organisation to disclose their personal information for direct marketing. This example makes sense if the individual's request were directed at the organisation that has the direct relationship with the individual, e.g., a bank, and goes towards our point that the Bill is targeted at consumer-facing service providers. However, were the individual's request to be made to an enterprise service provider (e.g., a carriage service provider) that the bank uses to send marketing and other communications to the individual, it could put the enterprise service provider at risk of potentially violating laws on telecoms intercept and/or its contractual obligations to the bank.

3.4. We therefore recommend incorporating an exception for enterprise service providers such that an organisation is not an OP organisation in respect of any service it provides where the service is:

3.4.1. primarily intended for use by another organisation, whether for the other organisation's own internal purposes or as an input to, or for the management, control or operation of, or to provide information about, one or more of the other organisation's services;

3.4.2. additional or ancillary to a service described in 3.4.1 above; or

3.4.3. enables end-users to engage only in private communications, including any oral or electronic communication.

In this respect, the term 'private communications' could be further defined as

any communication that is made by an originator who is in Australia or is intended by the originator to be received by a person who is within or outside Australia and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted without authorisation by any person other than the person intended by the originator to receive it.

Definition of social media services

3.5. The proposed definition for organisations providing social media services is

> ***6W Meaning of OP organisation***
>
> *Organisations providing social media services*
>
> *(1) An organisation is an **OP organisation** if the organisation:*
> *(a) provides an electronic service that satisfies each of the following conditions:*
> *(i) the sole or primary purpose of the service is to enable online social interaction between 2 or more end-users, including online*

[4] p. 6, Explanatory Paper, *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021*, Nov 2021

interaction that enables end-users to share material for social purposes;

(ii) the service allows end-users to link to, or interact with, some or all of the other end-users;

(iii) the service allows end-users to post material on the service;

(iv) such other conditions (if any) as are specified in a legislative instrument made under subsection (7); and

(b) is not specified in, or does not belong to a class of organisations specified in, a legislative instrument made under subsection (7).

(2) In determining whether the condition set out in subparagraph (1)(a)(i) is satisfied, disregard each of the following purposes:

(a) the provision of advertising material on the service;

(b) the generation of revenue from the provision of advertising material on the service.

3.6. This definition has to be read in context with the proposed definition of electronic service:

6X Meaning of electronic service

*(1) An **electronic service** is a service that:*

(a) allows end-users to access material using a carriage service (within the meaning of the Telecommunications Act 1997); or

(b) delivers material to persons having equipment appropriate for receiving that material, where the delivery of the service is by means of a carriage service (within the meaning of that Act).

*(2) Despite subsection (1), none of the following is an **electronic service**:*

(a) a broadcasting service (within the meaning of the Broadcasting Services Act 1992);

(b) a datacasting service (within the meaning of that Act);

(c) a service the sole purpose of which is to process payments;

(d) a service the sole purpose of which is to provide access to a payment system (within the meaning of the Payment Systems (Regulation) Act 1998).

3.7. Neither the term 'post' nor 'material' are defined in the draft Bill. However, it may be instructive to look at the definition of these terms in the Online Safety Act 2021 (OSA), given the similarity (or equality) of other definitions between the draft Bill and that Act. The OSA defines these two terms as follows:

5 Definitions

***material** means material:*

(a) whether in the form of text; or

(b) whether in the form of data; or

(c) whether in the form of speech, music or other sounds; or

(d) whether in the form of visual images (moving or otherwise); or

(e) whether in any other form; or

(f) whether in any combination of forms.

11 When material is posted by an end-user of a social media service, relevant electronic service or designated internet service

*For the purposes of this Act, material is **posted** on a social media service, relevant electronic service or designated internet service by an end-user if the end-user causes the material to be accessible to, or delivered to, one or more other end-users using the service.*

3.8. The Explanatory Paper aligns with the definition of electronic service in section 6X, where it notes: *"For the purposes of the OP code, the definition of 'electronic service' will capture a broad range of existing and future technologies, including hardware,*

software, websites, mobile applications, hosting services, peer-to-peer sharing platforms, instant messaging, email, SMS and MMS, chat services, and online gaming."[5]

3.9. However, because of the manner in which 'electronic services' is referred to in the definition of 'social media services', we are concerned that this could result in the definition unintentionally capturing a very large array of organisations who provide carriage services such as SMS, MMS, email and mobile applications, which are by their very nature services that allow for communication between individuals.

3.10. We note the RIS only assumes that 150 social media platforms would be captured by the reforms – a figure that would appear too low (if it is not too low already) if email, SMS, MMS, mobile applications, and other carriage services were included in the calculation.

3.11. We submit that the Bill and the Explanatory Memorandum both should make it clear that carriage services including SMS, MMS, email, and mobile applications do not fall within the scope of organisations providing social media services, as defined in section 6W.

3.12. The definition of 'social media services' should accordingly be amended to ensure that only organisations intended to be within the scope of the OP Code are captured.

3.13. We also note that the definition creates significant uncertainty as to whether services that provide chat features together with other features or functionality, such as online inter-player gaming, fall within the social or principal purpose test and therefore are regulated 'social media services'.

3.14. We recommend clarifying that the definition 'social media services' excludes carriage services (including SMS, MMS, email, and mobile applications) and services principally for online gaming where chat or other interaction between players or observers of player is a feature of the service. This could be achieved by incorporating an exception in a new subsection immediately after the existing subsection 6W(2) as follows:

> ***However, an organisation is not an OP organisation for the purposes of subsection 6W(1) to the extent that the electronic service referred to in paragraph (1)(a):***
> ***(a) is a carriage service (within the meaning of the Telecommunications Act 1997); or***
> ***(b) is an online gaming service and includes a feature that allows interaction between players or their observers.***

3.15. The Explanatory Memorandum should also be clear in discussing the scope of the Bill.

3.16. It is equally confusing that the Explanatory Paper counts messenger and videoconferencing services as social media services (Table 1 expressly lists "Online messaging and videoconferencing platforms such as WhatsApp and Zoom"[6]) when the OSA counted those services as 'relevant electronic services' (as opposed to social media services), although the OSA definition for social media services was identical to the one used in the draft Bill (with the exception of two missing clarifications, which we ask to be re-instated, and a slightly differently worded reference to other legislative instruments).

3.17. It appears flawed to capture the same service under one definition in one Act but to apply a different definition in another Act when the same definition is available and used in both pieces of legislation.

3.18. We argue that the definition of social media services ought to be amended to exclude the unintended services as described above. However, irrespective of such an

---

[5], p. 7, Explanatory Paper, *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021*, Nov 2021.

[6] p. 7, Explanatory Paper, *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021*, Nov 2021.

amendment, it would be more appropriate for messenger and video conferencing services to be covered by the definition of large online platforms, if necessary at all, in the context of this legislation.

3.19. We note that these definitional issues did not arise (although other definitional issues are a matter of concern) with respect to the OSA as that Act clearly juxtaposes social media services with relevant electronic services (under which email, SMS, MMS, messenger and videoconferencing services fall) and as most of the obligations under that Act equally apply to both of those categories of service providers.

3.20. In addition to the clarifications requested above, we also ask that the definition of social media services include the clarifying notes/sub-section that currently exist in the equivalent social media services definition in the OSA, namely:

[OSA definition reproduced below – clarifying notes/sub-section that should be incorporated in the Bill in ***bold***. The OSA definition is otherwise identical with the exception of sub-section 1(a)(iv).]

13 Social media service

(1) For the purposes of this Act, ***social media service*** *means:*

(a) an electronic service that satisfies the following conditions:

(i) the sole or primary purpose of the service is to enable online social interaction between 2 or more end-users;

(ii) the service allows end-users to link to, or interact with, some or all of the other end-users;

(iii) the service allows end-users to post material on the service;

(iv) such other conditions (if any) as are set out in the legislative rules; or

(b) an electronic service specified in the legislative rules;

but does not include an exempt service (as defined by subsection (4)).

Note: Online social interaction does not include (for example) online business interaction.

(2) For the purposes of subparagraph (1)(a)(i), online social interaction includes online interaction that enables end-users to share material for social purposes.

Note: Social purposes does not include (for example) business purposes.

(3) In determining whether the condition set out in subparagraph (1)(a)(i) is satisfied, disregard any of the following purposes:

(a) the provision of advertising material on the service;

(b) the generation of revenue from the provision of advertising material on the service.

Definition of data brokerage service

3.21. The proposed definition for data brokerage service in the draft Bill is as follows:

Organisations providing data brokerage services etc.

(3) An organisation is also ***an OP organisation*** *if:*

(a) the organisation collects personal information about an individual for the sole or primary purpose of disclosing that information (or information derived from that information) in the course of or in connection with providing a service (a ***data brokerage service****); and*

(b) the information:

(i) is collected by the organisation from the individual by the use of an electronic service, other than an electronic service covered by subsection (1); or

(ii) was previously collected by another organisation from the individual by the use of an electronic service, including an electronic service covered by subsection (1); and

(c) the organisation is not specified in, or does not belong to a class of organisations specified in, a legislative instrument made under subsection (7).

3.22. The above definition is overly broad, as there is no suggestion that the disclosure of the information (to a third-party organisation) is for money or money's worth. Such a broad definition could capture all organisations who are relying on other organisations to process information for them. As an example, the first organisation could be a school relying on the services of an email service provider to send emails to the school's students. It would lead to an absurd outcome for the school to be considered to be offering a 'data brokerage service'.

3.23. We therefore recommend ask that the language of paragraph 6W(3)(a) be adjusted as follows:

*(3) An organisation is also an **OP organisation** if:*

*(a) the organisation collects personal information about an individual for the sole or primary purpose of disclosing that information (or information derived from that information) **for monetary or other valuable consideration** in the course of or in connection with providing a service (a data brokerage service)."*

3.24. Additionally, there is substantial uncertainty as to whether the definition is intended to encompass data analytics services where relevant information is ingested (received or collected) in effectively anonymised form, that is then used to derive substantially transformed data analytics outputs, such as reports and insights, that are then made available to third parties only in effectively anonymised form. Capturing effectively anonymised data analytics outputs would not be consistent with 'trading in personal information', but is a likely result of the very broad proposed definition in section 6W(3)(a).

3.25. Consequently, the definition of 'data brokerage service' ought to be also amended to exclude the handling of anonymised information from the definition of 'data brokerage service'. We also note that the issue of anonymisation is a broader issue under consideration in the Privacy Act Review, and reiterate that consideration of the matters contemplated in the Bill ought to be delayed and considered together with or after the broader Privacy Act Review has been sufficiently processed.

Definition of large online platforms

3.26. The definition of large online platform, as currently drafted, appears to capture a wide array of organisations and platforms that are, so we believe, not intended to be within scope of the legislation.

3.27. The proposed definition of large online platform is as follows:

Large online platforms

(4) An organisation is also an OP organisation at a particular time in a year if the organisation:

(a) either:

(i) for an organisation that carried on business in the previous year—had, in the previous year, at least 2,500,000 end-users in Australia;

(ii) for an organisation that did not carry on business in the previous year—has in the current year at least 2,500,000 end-users in Australia; and

(b) collects personal information about an individual in the course of or in connection with providing access to information, goods or services (other than a data brokerage service) by the use of an electronic service (other than an electronic service covered by subsection (1)); and

(c) is not specified in, or does not belong to a class of organisations specified in, a legislative instrument made under subsection (7).

(5) However, an organisation is not an OP organisation for the purposes of subsection (4) to the extent that the organisation collects personal information about an individual in the course of or in connection with providing a customer loyalty scheme.

3.28. Along with the definition of 'electronic services' (previously referred to in this submission) the scope of large online platform is so broad it appears to cover a far greater number of organisations than that originally envisaged to be subject to an OP Code. In addition, the reference to end-user without a clear definition creates confusion.

3.29. The broad drafting would appear to apply to organisations who happen to collect personal information in the course of providing access to information, goods or services by use of an electronic service. This effectively means that any organisation with 2.5M end-users who uses any sort of online account management, SMS, MMS or mobile application services to engage with their users (all of which require the collection of some form of personal information) would be considered an OP organisation, regardless of whether there is any relevant use or disclosure of that personal information beyond a reasonable incident of dealing with an individual (i.e. supply a product).

3.30. This could include, for example, banking, insurance, energy, water, transport and aviation, post/delivery services, entertainment, as well as telecommunications providers. We believe all of these organisations primarily trade in goods or services that are not what would usually be understood to be 'online platforms'. Yet, because they may offer online or app-based account management services, such as, sales and order tracking, fault reporting, booking services, customer service chat capabilities, budget/spend or usage tools and management of marketing preferences (as required by law) they could come under the definition of a large online platform.

3.31. This is a fundamentally far broader scope than the type of organisations who were intended to be subject to the OP Code, as noted in both the Explanatory Paper[7] and Regulation impact Statement[8] accompanying the Bill.

3.32. It is, in our view, doubtful, whether much is to be gained from such a broad scope of services that either do not allow engagement with other end-users and/or target a very specific audience and purpose of low risk. The definition ought to be amended, beyond our proposed suggestions above, to ensure that low risk services are not captured within its scope.

3.33. Specifically, Communications Alliance considers the drafting of large online platform should be amended so that it is more clearly aligned with the intention for an OP Code. It should be clear that the definition of large online platform does not include telecommunications providers – i.e., those who provide services that can be used to access digital platforms. We suggest amending the exception to large online platforms in section 6W(5) in the following way:

[7] refer to p.4 and Table 1, and pp. 7-9, Explanatory Paper, *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021*, Nov 2021.

[8] p. 3 Enhancing online privacy and other measures, Early Assessment – Regulation Impact Statement, Oct 2021

However, an organisation is not an OP organisation for the purposes of subsection (4) to the extent that:

(a) the organisation collects personal information about an individual in the course of or in connection with providing a customer loyalty scheme; or

(b) the organisation supplies a carriage service.

Note: for the purposes of this section, carriage service has the meaning given to it in the Telecommunications Act 1997.

3.34. It is also unclear if messaging platforms would be considered an OP organisation; for example, organisations that provide appointment reminder messaging services (for example, to service providers, such as doctors, physiotherapists, dentists or hairdressers). The lack of clear definition for 'end-user' exacerbates this ambiguity. While the messaging service sends a communication to recipient (e.g. SMS appointment confirmation which may require a recipient to respond) the subscriber to the service is not the recipient of the message and the provider of the service does not have any customer relationship with the recipient of the message.

3.35. This ambiguity ought to be removed by clarifying the definition of end-user to mean active subscribers or registered users (as opposed to every person receiving, for example, a reminder SMS).

3.36. We accordingly recommend inserting a definition for "end-user", in the context of defining 'large online platforms' as follows:

For purposes of section 6W, subparagraphs (4)(a)(i) and 4(a)(ii) end-user means a person who has established and currently maintains an active account directly with the relevant organisation and who must authenticate their identity prior to accessing or using their account.

3.37. It is also important to note that any organisation covered by the definitions of social media service and large online platforms will be regulated by the OP Code for all its services and activities and not only those that have given rise to the organisation being subject to the regulation in the first place. This is also problematic and does not strike the right balance between the need to enhance privacy protections and the regulatory burden imposed.

3.38. Companies have often sought to have customer service and account management available and easily accessible to customers (indeed there is a current push to digitise the Australian economy). Online accounts, mobile applications, SMS, email and MMS communications have been a significant part of many companies' efforts to reduce costs, increase timely communication and give improved access and control to their customers over their services and relevant information. It allows simple customer needs to be actioned promptly and is part of better customer service.

3.39. Overall, in our view, the scope of the definitions is disproportionate to the stated aim and does not align with the intent promulgated by Government.

Exemption of loyalty schemes from the scope

3.40. Section 6W(5) of the draft legislation sets out than an organisation is not an OP organisation "… *to the extent that the organisation collects personal information about an individual in the course of or in connection with providing a customer loyalty scheme*". As noted above, once an organisation is captured under the definition of large online platform and uses an electronic service, it would appear to be regulated under the OP Code for ***all*** its products and services. The drafting of section 6W(5) creates confusion, as it excludes an organisation that runs a loyalty scheme from being regulated by the OP Code but only in relation to the loyalty scheme (i.e., only to "*the*

extent" the organisation collects personal information in relation to the loyalty scheme).

3.41. Some Communications Alliance members run loyalty schemes (also known as rewards programs).[9] The exclusion of the loyalty scheme (section 6W(5)) creates significant challenges for any organisation that also runs a loyalty scheme (as some aspects of the collection and use of personal information will fall under the OP Code, whereas the same personal information in the context of the loyalty scheme does not fall under the remit of the OP Code), and will also create confusion for consumers who are likely to consider that their personal information is handled in a consistent manner by an organisation.

3.42. The Explanatory Paper only states that "Customer loyalty schemes are being considered as part of the Privacy Act Review."[10] No further policy reason is being provided that would justify why loyalty schemes are being afforded an exclusion from this Bill when many other services are also being considered as part of the Privacy Act Review.

3.43. The primary purpose of a loyalty scheme is the collection of data on the browsing and purchasing habits of the customers subscribed to the scheme to further future sales. In addition, many loyalty schemes have many millions of subscribers.

Consequently, we strongly recommend further consideration is given to how loyalty schemes are either captured or excluded from the OP Code, and we consider this is best done holistically as part of the Privacy Act Review, rather than through an expedited OP Bill that risks fragmentation and confusion, as we explained in section 2 of our submission.

Undue focus on organisations instead of the activities that those organisations undertake

3.44. Each OP organisation is covered and regulated for all of its activities, not only for the provision of a service that led to the organisation becoming within coverage.

3.45. The only exception (outside the exercise of Ministerial discretion) is in the event that section 26KC(9) is used by the code developer or the Commissioner to exclude from coverage particular activities of a covered entity as specified by the code developer or the Commissioner, respectively.

3.46. This leads to clear inequity between specialist entities and diversified entities and makes it much less likely that potentially covered entities will be able to negotiate and reach agreement on a code. The range of activities that will need to be taken considered in drafting of the code is huge. This makes it much more likely that the Commissioner will need to determine a code.

3.47. Importantly, it is a disproportionate response to policy-relevant concerns as articulated by the Government to date.

3.48. Consequently, we submit that the OP code should cover acts and practices in collection and handling (including disclosures) of personal information in relation to an activity that is (newly defined as) a covered activity as per the (amended and clarified) definitions above, where that information is directly or indirectly derived from the conduct of that activity.

[9] For example, Telstra runs Telstra Plus, https://plus.telstra.com.au/

[10] p. 8, Explanatory Paper, *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021*, Nov 2021

4. Expansion of notice requirements for all OP organisations

Unintended interaction between section 26KC(2)(c) and the APPs for notification

4.1. The Discussion Paper canvasses substantial revisions of existing APPs which address required coverage of privacy policies and privacy notices respectively.

4.2. By the OP Bill, these existing APPs must be addressed and elaborated upon by the OP code. These code provisions will then need to be revisited and revised when these APPs are changed by a revised Privacy Act.

4.3. The most relevant APPs in this context are:

- APP 1.4(c) about privacy policies: the OP code must set out how an OP organisation's APP privacy policy is to state the purposes for which the organisation collects, holds, uses and discloses personal information.
- APP 5.2 about privacy (collection) notices: the OP code must set out how an OP organisation will give notice to individuals about collection of personal information, as well as how an OP organisation will give notice to individuals in compliance with a new requirement mandating an OP organisation to notify an individual, or to otherwise ensure that the individual is aware, of the purposes for which the organisation collects, uses and discloses personal information.

4.4. The intended scope of operation of the proposed new requirement as to notification of purposes is most unclear, noting that existing APPs 1.4(c) and 5.2(d) already directly address notification of purposes.

Section 26KC(2)(c) may be read as significantly broadening the range of circumstances in which notice must be given to individuals as to purposes of collection and handling, and as to other matters as addressed in APP 5.2.

4.5. Given the aforementioned processes on foot, this is an inappropriate and substantial extension to currently legislated requirements as to privacy notices. Consequently, section 26KC(2)(c) should be deleted.

Notifying conduct constituting interference with privacy of individual (Section 52A(1)(c))

4.6. Under the proposed new section 52A, when the OAIC investigates a complaint under section 52(1), or investigates an act or practice that may be an interference with the privacy of an individual or APP 1 (section 52(1A)) and finds it to be substantiated, the OAIC's determination may now also include a declaration requiring the respondent to prepare and publish (or otherwise communicate) a statement setting out a description of the conduct that constitutes the interference with the privacy of an individual **and the steps (if any) undertaken** or to be undertaken by the respondent to ensure that the conduct is not repeated or continued.

4.7. We are concerned that publishing details of specific steps undertaken (or yet to be undertaken) by the respondent risks providing information to cyber criminals that may help them find vulnerabilities or alternate ways to compromise a system. We note the declaration can require the respondent to set out the conduct and the steps taken or to be taken to ensure it does not happen again (as well as anything else in the declaration (s.52A (1a)(iv)). While we appreciate that there is a reasonableness condition (s.52A(2)), our concern is where an APP entity has to publish (s.52A (1c)) more broadly a statement describing a vulnerability which caused the breach and it has not yet taken the steps required in the declaration, this could highlight this vulnerability to criminals. The same applies if the organisation describes new remedial internal processes which may be used by criminals to identify additional vulnerabilities.

4.8. We consider that if the entity has already informed the relevant impacted individuals of what it is doing to rectify a privacy breach, broadcasting it any more widely potentially only risks informing cyber criminals with very little benefit for consumers in general.

5. Expansion of consent requirements for all OP organisations

5.1. APP 3 and 6 currently address when and how consent must sought for certain specified collections, uses and disclosures of personal information.

5.2. Section 26KC(2)(e) goes beyond requiring the code to set out how an OP organisation is to comply with these (existing) APPs, and states that the code must make provision addressing the providing of consent, including "*the circumstances in which consent is taken to be provided voluntarily, and is informed, unambiguous and specific; and consent is taken to be current […]*".

The scope of operation of the proposed new requirement as to consent is clear and substantial, noting that existing law as to consent generally allows inferred consent and does not require consent for many acts and practices in collection and handling of non-sensitive personal information.

5.3. APPs 3 and 6 already directly address circumstances in which consent must be sought and obtained, and the definition of 'consent' and associated OAIC guidance addresses current requirements as to obtaining (valid) consent.

5.4. Section 26KC(2)(e) may be read as significantly broadening the range of circumstances in which consent must be sought and obtained, and expressly overriding the current definition of 'consent' and associated OAIC guidance as to requirements for valid consent.

5.5. There is a significant risk that this provision could be used (for example, by the Commissioner in mandating a code) to (1) significantly broaden the range of circumstances in which consent must be obtained, and (2) require unambiguous affirmative express consent in all such circumstances, and without any carve-downs or exceptions for legitimate uses/interests, compatible uses or like carve downs.

5.6. In line with our comments above, we believe that this is an inappropriate and substantial extension to currently legislated requirements as to consent, and consequently, section 26KC(2)(e) should be deleted from the draft legislation.

5.7. Overall, it is worth highlighting that the range of proposed matters required for inclusion in the OP code (as listed in subsection 26KC(2)) has not been demonstrated as requiring urgent coverage, particularly in relation to OP organisations that are not social media platforms.

Government has acknowledged a much lower risk of privacy harms in respect of activities of organisations that are not social media platforms as compared to provision of social media services., Therefore, it is unclear why section 26KC(2) would be required at this stage, if at all. If changes to notice and consent requirements are necessary, these ought to be implemented as part of the larger review and on an economy-wide basis.

6. Age verification and parental/guardian consent

Age verification

6.1. Section 26KC(6) of the draft Bill provides that the OP code must require social media services as defined in the draft Bill (among other things) to

(6) Without limiting subsection (5), the OP code must require OP organisations of a kind covered by subsection 6W(1) to do the following:

(a) take all reasonable steps to verify the age of individuals to whom the OP organisation provides an electronic service;

(b) obtain the consent of a parent or guardian of a child who has not reached 16 years before collecting, using or disclosing personal information of the child;

(c) if the OP organisation becomes aware after it collects, uses or discloses personal information of an individual that the individual is a child who has not reached 16 years, obtain the consent of a parent or guardian of the child as soon as practicable after becoming so aware;

(d) take all reasonable steps to verify the consent obtained for the purposes of paragraph (b) or (c);

6.2. We object to age verification requirements being contained within the Bill. As the Office of the eSafety Commissioner correctly indicated in a recent Roundtable on the AVR, age verification is a highly complex and controversial subject which requires substantial analysis of existing and future technical capabilities, the respective advantages and potential unintended consequences of the tools on the market or currently under development, and discussion with industry players. The Office of the eSafety Commissioner called it a 'feasibility study including a study of implementation timeframes'.

Noting that this 'feasibility study' by the Commissioner will not be concluded prior to December 2022 (which is an appropriate timeframe given the complexity of the task at hand), it is inappropriate for the Bill to require the code to prescribe age verification measures.

6.3. It is worth noting that the UK Information Commissioner recently published her Opinion on Age Assurance for the Children's code. In her Opinion, the Commissioner cautioned organisations that:

"age assurance must be used carefully as it carries its own types of risk. For example, it:

- *may be disproportionately intrusive. For example, age verification checks often require access to official data or documentation which can include special category data;*
- *may introduce risks of bias and inaccuracy. For example, some emerging approaches to age estimation are based on profiling or facial analysis using AI;*
- *may result in exclusion or discrimination of already marginalised groups due to bias, inaccuracy or requirements for official documentation. Those in more deprived socio-economic groups are more likely to lack requisite documentation, and more likely to be affected by algorithmic bias. Non-white ethnicities and people with disabilities are over-represented in these groups. Individuals may be unable to use some types of age assurance due to physical or cognitive reasons and risk being excluded from services they are entitled to access;*
- *is not fool-proof. Any approach has some risk of incorrectly classifying a child as an adult or as an older child. This could potentially allow them access to inappropriate or harmful services or material. Conversely, an adult may be incorrectly classified as a child, and be denied access to services they are legally entitled to use; and*

- *some methods can be circumvented. For example, a child or parent could provide false information in a self-declaration or a child could log into their parent's account to complete account confirmation."*[11]

The UK Information Commissioner further notes that age verification measures are currently *"primarily used by sites that provide goods or services that attract criminal or civil penalties for serving underage customers: online retailers who sell age-restricted products, for example alcohol, tobacco products including vape, and knives."* [12]

Importantly, the UK Commissioner recognises that *"Most age verification services cannot be readily used to determine the age of a child as they only provide confirmation that the data subject is over or under 18. It is not a solution for age-appropriate design elements such as tailored transparency or nudging. Age verification could be used to determine age based on documentation, but this would be highly intrusive."*[13]

6.4. In the above, we have highlighted the potential unintended consequences of age verification more generally, and usually with a view to distinguishing a child (a minor of less than 18 years of age) from an adult. Many of the aforementioned difficulties become more pronounced when age verification is attempted for children, e.g. at the age of 16, as proposed by the draft legislation. One reason for this lies in the fact that children are less likely to have identity documentation.

6.5. Importantly, age verification is contrary to the aim of data minimisation, i.e. it is likely to force social media platforms to collect and store more data (or access a third party's data which they normally would not access). These organisations may also become the target of malicious actors. In any case, the outcome appears counterproductive to the stated aim of improved privacy protections for children.

6.6. As previously indicated, the costs associated with age verification are substantial, if not exorbitant, i.e. the RIS estimates the costs associated with age verification and parental consent will account for 99% of the costs associated with the implementation and running of the scheme at around $526 million. As stated above, in our view, it is impossible to justify this expense given the current state of debate around age verification. It should also be noted that the substantial costs associated with age verification would need to be borne by all social media service providers, regardless of their size. This may significantly stymie competition as it is, typically, much harder for smaller providers to bear larger regulatory costs and required capital investments than this is the case for larger players.

6.7. Consequently, we recommend that the term 'age verification' be replaced with 'age assurance', thereby allowing social media services the necessary degree of flexibility to implement measures that do not unintentionally disadvantage children, vulnerable user groups or otherwise negatively impact on the privacy of the users of their services.

6.8. We also believe that section 26KC(6)(a) should be amended in two respects:

1. **only require social media service providers to take 'reasonable steps' (as opposed to 'all reasonable steps') in relation to age assurance: it is not useful to require that <u>all</u> reasonable steps be taken as long as the provider has achieved the desired outcome that it can be reasonably assured that the individual is of the required age to use the service. It is also not easy to determine what 'all reasonable steps' would include at a specific point in time, and certainly not dynamically with evolving technology and new tools for age assurance progressively becoming available.**

---

[11] pp.10/11, UK Information Commissioner, *Information Commissioner's opinion: Age Assurance for the Children's code*, Oct 2021

[12] p135, UK Information Commissioner, *Information Commissioner's opinion: Age Assurance for the Children's code*, Oct 2021

[13] ibid

2. **require taking those reasonable steps in relation to age assurance for individuals to whom they are providing the respective social media service (as opposed to any electronic service as currently drafted): social media services may provide other electronic services (noting the very broad definition of electronic services) that are unrelated to their social media services. Age assurance measures ought not be required for those services but only for the social media services that are the focus of the respective harm prevention measures.**

Age threshold of 16 years

6.9. The draft Bill proposes an age threshold of 16 years, below which parental consent is required prior to the collection, use or disclosure of personal information of the child.

6.10. The Discussion Paper does not provide a policy rationale or any research or data as to why specifically this age has been chosen. However, the Discussion Paper does highlight that OAIC provides guidance that organisation "*may presume that an individual over the age of 15 has the capacity to provide consent to collection, use or disclosure of personal information unless something suggests otherwise.*"[14]

6.11. The Paper then goes on to say: "*The Bill will elevate protections for children and vulnerable groups by including stronger and more robust privacy protections as requirements in the OP code, as opposed to guidance.*"[15] While this statement in and of itself is problematic, it does not provide any indication as to why the age threshold of 16 years – deviating from the OAIC's guidance – has been chosen specifically to apply to social media services.

6.12. The age threshold of 16 years appears arbitrary and is inconsistent with other approaches to consent. It appears that the balance in relation to other freedoms and responsibilities has not been struck appropriately.

6.13. For example, with respect to medical treatment the legislation adopts an approach for non-emergency treatment that rests on the concept of a 'Mature Minor':

> "*Generally, a Minor is capable of independently consenting to or refusing their medical treatment when they achieve a sufficient level of understanding and intelligence to enable them to understand fully what is proposed. This means that there is no set age at which a child or young person is capable of giving consent. […] For example, it may be likely that a 15-year-old would be assessed as having the capacity to consent to receive contraceptive treatment.*"[16]

This means that a minor is likely to obtain some medical treatment, including contraceptive treatment, without parental consent (we use parental consent as a short form for parental and guardian consent) but would, if the Bill was enacted, be unable to obtain a social media account without parental consent.

6.14. In a similar vein, in all Australian jurisdictions the criminal age of responsibility remains at only 10 years[17] despite the United Nation's Universal Period Review's recent calls to raise Australia's criminal age of responsibility to 14 years of age, in line with most other advanced economies.

6.15. Consequently, as of 14, minors may be held fully responsible for their actions (but are subject to a different range of sanctions than adults committing the same offences),

---

[14] p.11, Explanatory Paper, *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021*, Nov 2021

[15] ibid

[16] from: https://www.health.nsw.gov.au/policies/manuals/Documents/consent-section-8.pdf accessed on 01/12/2021

[17] the *doli incapax* presumption applies between the ages of 10-14, a short discussion of the matter can be found here.

and yet would be unable to subscribe to a social media service if this required the collection of their name or email address. This seems disproportionate.

6.16. We believe that the Bill ought not to prescribe age assurance for a specific age. Instead, it should require social media services to take the reasonable assurance measures for the age for which the service is designed, i.e. for some services, this will mean age assurance and parental consent measures (however, refer to our comments around parental consent further below) at e.g. 13 years of age while other services may attract such measures at 16 years. Providers could report to the eSafety Commissioner which respective services they offer, including their relevant features and age limits.

This would strike an appropriate balance between the desired privacy protection of children, children's abilities to understand their actions (and consequences) with increasing age and delegation to parental supervision (through consent) where required.

Not doing so risks pushing children under the age of 16, who do not want to seek parental consent, to less well moderated platforms operated by organisations without an Australian presence that may choose not to comply with some or any requirements of the Bill. In addition, some organisations may choose not to establish an Australian presence and disengage with investment in Australia in order to minimise legal risk and on the assumption that it will be harder to take enforcement action against their practices without such presence/engagement.

Verification of parental/guardian consent

6.17. Section 26KC(6)(b) draft Bill requires that the OP code impose a duty on social media service providers to obtain parental/guardian consent of a child of under 16 years prior to collecting, using or disclosing personal information of that child.

6.18. Section 26KC(6)(c) stipulates the retrospective collection of such consent as soon as practicable after becoming aware of the collection, use or disclosure of personal information of a child, i.e. of existing users of a service that are currently younger than 16 years where the provider becomes aware of their younger age.

6.19. Importantly, Section 26KC(6)(d) asks providers to "*take all reasonable steps to verify the consent obtained*" [emphasis added] from parents/guardians.

6.20. Our concerns in relation to the verification of parental consent are similar to those of age verification. However, in addition to the latter, it is unclear what form of documentation would be acceptable or required to prove a child's familiar relationship (or guardianship arrangements). In any case, it seems clear that a significant amount of personal information, that may not be readily at hand, may need to be disclosed.

6.21. Consequently, in line with our recommendations above, we advocate for social media service providers taking 'reasonable steps' (as opposed to 'all reasonable steps') to satisfy themselves of parental/guardian consent at the age that is appropriate for the respective service (see Sections 6.7, 6.8 and 6.14 above).

7. Opt-out of disclosure and use of personal information

7.1. Section 26KC(2)(h) requires the OP code to

> "*subject to subsection (3), make provision for or in relation to requiring OP organisations to take such steps (if any) as are reasonable in the circumstances to not use or disclose, or to not further use or disclose, the personal information of an individual if so requested by the individual.*"

7.2. The opt-out in section 26KC(2)(h) is stated in the Explanatory Paper as "not intended to be a right of erasure", but is noted as a blanket right as to cessation of use or disclosure of 'personal information of an individual' and accordingly covers all uses of first party data and is not directed at disclosures of first party data (then becoming third party data in the hands of a recipient) for use by the recipient for targeting or other online marketing.

7.3. We believe that the provision should not include uses of first party data where there is no disclosure of this data to a third party in a form where an individual is reasonably identifiable by that third party.

7.4. The current drafting also does not clearly carve out uses or disclosures of derivative information that through deidentification processes or practices have ceased to be 'personal information about an individual', whether under existing definitions or as the *Privacy Act 1988* may be revised.

As drafted, the opt-out would apply to any and all uses and disclosures of personal information about any individual, and not only uses for targeted advertising or other direct marketing, and not only profiling of identifiable individuals.

7.5. This is a broader scope of coverage of opt-out than that tentatively endorsed in the Discussion Paper.

This opt-out is qualified only by "*such steps (if any) as are reasonable in the circumstances*". This qualifier will be practically impossible to give effect to in the OP code, because of the range of activities and range of entities to whom the Government proposes that the code relates. It is not clear what may be regarded as reasonable bases for exceptions from an opt-out option (i.e., carve-downs for reasonably anticipated or compatible uses or legitimate uses or interests).

7.6. The consequences of the current drafting, i.e. the ability for customers to opt out of <u>all</u> advertising (as opposed to personalised advertising) are not of theoretical nature but pose very real challenges as the lack of advertising revenue may make the operation of a service commercially unviable or may require the transformation of the service from a free offering to a subscription service.

7.7. Importantly, where services use personal information to target content delivery to the specific age group and preferences expressed by users, such content delivery would not longer be possible once an individual has opted out of all personal information being used. As a result, the individual may receive content unsuitable for their age or out of step with their indicated preferences.

7.8. Consequently, such an uncertain and broadly drafted opt-out should not now be required in advance of the legislature enacting reforms as canvassed in the Discussion Paper and section 26KC(2)(h) should be deleted.

As a result, sections 26KC(3) and (4) would be redundant and should also be deleted.

If opt-out is required now for inclusion in an OP code, section 26KC(2)(h) should focus on opt-out from disclosure and use for specific products or services that the provider offers and be limited to those products/services where the personal information is not required for the provision of the service.

8. Extraterritorial application

8.1. Section 5B of the *Privacy Act 1988* makes the following provisions for organisations and small business operators in relation to extraterritorial application

> "*(1A) This Act, a registered APP code and the registered CR code extend to an act done, or practice engaged in, outside Australia and the external*

Territories by an organisation, or small business operator, that has an Australian link.
Note: The act or practice overseas will not breach an Australian Privacy Principle or a registered APP code if the act or practice is required by an applicable foreign law (see sections 6A and 6B)

Australian link

(2) […]

*(3) An organisation or small business operator also has an **Australian link** if all of the following apply:*

(a) the organisation or operator is not described in subsection (2);

(b) the organisation or operator carries on business in Australia or an external Territory;

(c) the personal information was collected or held by the organisation or operator in Australia or an external Territory, either before or at the time of the act or practice." [emphasis added]

8.2. The draft Bill proposes to repeal paragraph 5B(3)(c).

The Explanatory Paper notes as the reason for the proposed deletion:

> *"[…] when a breach of the Privacy Act occurs, it may be difficult to establish that these foreign organisations collect or hold personal information from a source in Australia. This is because large multinational companies may collect personal information from Australian customers from an entity that is not incorporated in Australia, and transfer it to other entities overseas for processing and storage. Similarly, foreign organisations may collect personal information about Australians but do not collect Australians' information directly from Australia, and instead collect the information from a digital platform that does not have servers in Australia and may therefore not be considered 'in Australia'.*

The Bill will remove the condition that an organisation has to collect or hold personal information from sources inside of Australia. This would mean that foreign organisations who carry on a business in Australia must meet the obligations under the Privacy Act, even if they do not collect or hold Australians' information directly from a source in Australia. For example, an organisation that collects personal information of Australians from a digital platform that does not have servers in Australia will more clearly be subject to the Privacy Act."[18]

8.3. However, the repeal of paragraph 5B(3)(c) would have far greater consequences as it reduces the 'Australian link' requirements – which trigger the extraterritorial application of the Act and registered codes – to effectively only one limb: to carry on business in Australia or an external Territory.

8.4. This would leave general Australian law as to interpretation of statutes which do not have express exterritorial provisions to determine the extent to which a non-Australian entity that carries on business in Australia is regulated in relation to acts and practices in handling of personal information of individuals that are outside Australia.

General Australian law does not provide clear guidance to enable the coverage of this amended provision to be reliably assessed.

8.5. The Act should continue to have the second limb, such that an organisation has to collect or hold personal information from sources inside of Australia. If the concern is that an organisation may indirectly collect or hold information that is derived from another source within Australia that directly collects or holds the information, section 5B could be amended to bring such indirect collection and holding within the definition. Otherwise, the change would create broad, uncertain and unconstrained

[18] p.22/23, Explanatory Paper, *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021*, Nov 2021

extraterritoriality that is not consistent with good legislative practice and comity between national laws.

9. Code development

9.1. Communications Alliance and other industry associations are currently collectively developing Online Safety code/codes as intended by Parliament under section 137 of the OSA. The time allowed for this process is effectively 12 months, which may be stretched to 18 months if two codes are being developed, where 'code 1' is to deal with the most egregious forms of content first (and by the 12 months deadline).[19]

9.2. The timeline for the registration of the Online Safety code(s) is ambitious, to say the least, and involves a very large amount of resources and coordination across (currently) six industry associations.

9.3. Yet the broad scope of the proposed requirements means it potentially applies to multiple disparate industries. It could potentially cover industries such as banking, insurance, energy, transport and aviation, postal/delivery services, entertainment and telecommunications, just to mention a few. We anticipate that the process for the development of the OP code, which requires involvement across a far greater range of sectors and covers (as per the current draft Bill) substantial areas of reform, would require at least the same amount of time and resources, if it is workable at all.

Consequently, the draft Bill ought to state a realistic timeframe for the minimum timeframe for code development and registration. The 120 days proposed in section 26KE(3)(a) ought to be amended to 12 months. The fact that the Commissioner may extend the minimum period is as such not an argument to stipulate a period that is completely unrealistic to start with.

10. Commissioner's power to appoint an adviser

10.1. The draft Bill proposes to amend section 52(1)(A) of the Privacy Act 1988 to include a power for the Commissioner to request that an organisation appoint a 'suitably qualified independent adviser'. In addition, the appointment of the adviser has to occur in consultation with the Commissioner.

10.2. The only threshold test for the Commissioner has to satisfy in relation to the request of appointment of an independent adviser is that the request must be "reasonable and appropriate" (section 52(1)(AA)).

10.3. This power, which can be exercised following any complaint, is extraordinary. We recommend that the power be limited to serious breaches and/or be restricted to instances of repeated breaches where the Commissioner has formed a view that such an appointment is necessary to prevent further breaches.

For determinations which are not for serious and/or repeated breaches, it may be appropriate to add an obligation for the entity to engage in ongoing reporting directly to the regulator to provide transparency.

11. Disclosure of information

Sharing information with overseas regulators

11.1. We take the view that the Commissioner's sharing of information and documents with foreign authorities, as proposed in the new section 33A of the *Privacy Act 1988*, may

[19] Refer to p.76 of the eSafety Commissioner's Position Paper *Development of industry codes under the Online Safety Act*, Sept 2021

undermine, in some instances, due process as it may enable a foreign authority to circumvent established rules and principles in its respective jurisdiction in order to obtain information and/or documents. Where possible, foreign authorities should rely on their local powers to compel information.

11.2. We recommend that the Bill ought to be amended to include a provision to require the Commissioner to provide notice to the entity and provide the entity an opportunity to object to the sharing with a foreign authority, prior to any disclosure to an overseas authority.

We would also suggest further limitations are put in place with respect to what can be shared. For example:

1. **For the purpose of cooperation only information can be shared (not documents); and**
2. **Information and documents can only be shared where the Commissioner is transferring a complaint or part of a complaint to the foreign authority.**

Public interest disclosures

11.3. The proposed section 33B(1) would empower the Commissioner "*to disclose information acquired by the Commissioner in the course of exercising powers, or performing functions or duties under this Act if the Commissioner is satisfied that it is in the public interest to do so.*"

11.4. Section clause 33B(4) contains the proposed public interest test, i.e. that the Commissioner must have regard to:

(a) the rights and interests of any complainant or respondent;
(b) whether the disclosure will or is likely to prejudice any investigation the Commissioner is undertaking;
(c) whether the disclosure will or is likely to disclose the personal information of any person;
(d) whether the disclosure will or is likely to disclose any confidential commercial information.

11.5. There is no limitation as to the nature of information that may be disclosed and, accordingly, disclosed information might include any information supplied to the Commissioner in the course of an investigation, regardless of whether that information is contested as to accuracy, completeness or relevance.

11.6. Equally, no requirement exists for prior consultation with the person or entity that provided the relevant information or to whom the information relates.

11.7. There is also no requirement for the Commissioner to consider proportionality or to balance the benefit to person or entity that provide the relevant information or to whom the information relates against any detriment of disclosure. The Commissioner only needs to 'have regard' to such things.

11.8. Moreover, there is also no guidance as to how the Commissioner determines what is (or is not) in the public interest.

11.9. Consequently, we recommend that section 33B(1) be amended to include these reasonable and minimal safeguards.

12. Transparency in rule-making

12.1. There are various powers granted to the Minister and the Commissioner under the Bill to designate organisations as OP organisations and to make determinations on whether organisations have breached the registered OP code, among others. However, there

does not appear to be any requirement for either the Minister or the Commissioner to consult the public prior to exercising such powers.

12.2. In the interest of transparency and due process, we ask that the Bill be amended to incorporate requirements for good-faith public consultations of appropriate durations to be conducted prior to:

- **the Minister making any specification under section 6W(7) of the Bill (specifying conditions for an organisation to be considered a social media organisation, or specifying organisations or classes of organisations as social media organisations, data brokers, or large online platforms); and**
- **the Commissioner making any public interest determinations or temporary public interest determinations under Part VI of the Bill.**

13. Conclusion

Communications Alliance looks forward to continued engagement with the Department and other relevant stakeholders on ensuring that all Australians' privacy, especially that of younger Australians, is adequately protected.

However, we believe that the timing of the Bill and subsequent code creation is unworkable, the proposed scope of organisations captured by the Bill does not align with the stated intent and raise concern that some of the measures may be impractical, inappropriate or counter-productive to the stated aim of privacy protection.

We continue to lend our support to the overarching objectives of the Privacy Act Review and stand ready to work with all stakeholders to facilitate an effective and efficient adoption of a new, economy-wide privacy regime.

For any questions relating to this submission please contact Christiane Gillespie-Jones on 02 9959 9118 or at c.gillespiejones@commsalliance.com.au.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E
info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507